Global Information Assurance Certification Paper

Secure eMail

Determining an Enterprise Strategy and Direction

- Marian B. Gurowicz

- GIAC Security Essentials Certification (GSEC)
- Version 1.4 (amended April 8, 2002)
- Option 1
- Original Submission
- SANS 2002 Orlando

Secure eMail

Determining an Enterprise Strategy and Direction

TABLE OF CONTENTS

Secure eMail

ABSTRACT

Secure eMail has become a buzzword in business these days. But much like the current magazine advertisement that states: "I just told management the Firewall was secure. (Translation: Do we have a firewall?)," no one is quite sure what secure eMail is.

This paper will provide the security professional with the research needed for starting a secure eMail project and putting together a management proposal for a secure eMail solution. It will cover:

- Determining whether a business need for secure eMail exists in their company
- Defining the requirements that must be met in order to meet those needs
- Understanding the differences in the products that are offered as secure eMail solutions.
- Performing an in depth analysis of what is currently available in the market

INTRODUCTION

It wasn't that long ago, a business' primary means of communication with its customers, clients, business partners and employees, consisted of telephone, fax or paper documents that needed to be delivered. In recent years, the emergence of web technology and electronic communication has caused many businesses to re-evaluate the most effective and efficient means of communication.

Unfortunately, with the arrival of this new technology a new breed of menace has also appeared. From the bored to the financially challenged, many have found a way to subvert the intended use of modern technology: some for simple acts of vandalism, some just to prove they can, and some for financial gain. To the company that is attacked, however, the reason behind it has little meaning. They are left to deal with the financial losses, customer desertions and damage to professional reputation that being subjected to such an attack entails.

In the pages that follow, we will deal with just one application of new technology, eMail, and the safeguards that companies must take. As in all aspects of Information Security, the three fundamental principles of Confidentiality, Availability and Integrity are essential to the process of defining needs. In eMail security, there is another principal to consider as well: Non-repudiation or that the creator and/or sender of the information cannot later deny their intention to create or transmit the information.

We will take a look at how each of these principles will influence the decision in what type of security is needed. We will also touch briefly on balancing cost to risk. And then look at what is currently available.

DEFINING SECURE EMAIL

The most common analogy one sees and hears when researching the risk inherent in eMail, is that it is the equivalent of sending a postcard through the U.S. mail. It can be viewed, diverted based on content and/or altered. This is only part of the story of what can go wrong.

Secure eMail means that the sender can be assured that the message sent will be delivered to the intended recipient without interference, changes or disclosures to any third parties. It also means that the recipient can be certain

that the sender named is indeed the person who sent it, that the content is the same content that was originally entered, that no one has viewed it in transit and that no one has added any surprise payloads.

Or to put it another way:

> *Plain email is not a secure medium. Messages can be read by people with authorized (or unauthorized) access to mail servers which handle the mail, unlikely though this might be. There are a few basic requirements for secure and private exchange of email:*
>
> - ***Confidentiality** nobody other than the intended recipient can read the message;*
> - ***Integrity** we know that a message hasn't been tampered with in transmission.*
> - ***Authentication** we can be certain that the message comes from the person from whom it appears to come;*
>
> *Where privacy, authenticity and integrity of information sent is vital, users will look for ways of making their email secure. There are a number of tools and standards available for the secure and private exchange of email, though unfortunately they don't necessarily interoperate with each other.* [1]

When considered in this light, the predictable management response is "Secure it!" Now the security professional is left with the daunting task of determining how.

DEFINING THE NEED

The natural starting point for a project involving new technology is a search of the Internet, however, if one were to type "Secure eMail" at any search engine there would be easily 3 million hits. Just for argument's sake, assume one could evaluate and gather the information needed from each reference in one minute. It would still be a job that would take 24 years without vacation, holidays or days off just to sort through the information currently available.

One must obviously narrow the parameters before attempting any research.

[1] Isaacs, Margaret. "Security and Encryption -- Secure email." Terena Guide to Network Resource Tools. 21 Aug 2002. http://www.terena.nl/libr/gnrt/security/s4.html (16 Sep 2002)

Although the management directive may have been to "secure it", the first step is to define what "it" is and whether "it" really needs to be secured. For example, a company whose definition of eMail is an internal messaging system not connected to the Internet that is only used for employee convenience probably has no reason to proceed. On the other hand, a large financial institution that uses Internet eMail to correspond with customers and vendors on confidential matters or that receives eMail from external sources, whether as part of its business or external messages to employees may be at risk.

A good place to start is with the published corporate eMail Policy. Keep in mind that published policy does not always agree with what happens in the field. Both the stated and actual eMail usage need to be documented with respect to frequency, volume, content and recipient. One also needs to be aware of the change in usage that could be expected if a secure method of eMail delivery were made available.

Frequency refers to the regularity of eMail correspondence with another party. Volume would be the total number of eMails sent on a regular basis. The solution for a company that is mailing 365 eMails to different people on one day would be different than for a company that is sending one person a daily message.

Content will be used to assess the risk involved in a message that was compromised. If the only potential breaches in security would result in no personal or financial damage, the implementation of a Secure eMail Solution is not warranted. However, if a single breach could result in a million-dollar loss, it might. It will be for management to determine their risk tolerance; it will be up to you to present them with the facts.

Finally, the recipient will help you determine if the issue must be addressed from the internal network or as Internet eMail that crosses public lines.

Additionally, certain industries may have requirements mandated by the government. For example:

> *The Gramm-Leach-Bliley Act (GLBA), also know as the Financial Instituion Privacy Protection Act of 2001, requires that financial services firms maintain the security and privacy of NPI (Nonpublic Personal Information) about their customers. NPI includes:*
>
> - ✓ *Fact that an individual is the customer of a particular financial institution*
> - ✓ *Consumer's name, address, social security number, account*

number

- ✓ *Any information a consumer provides on an application*
- ✓ *Information from a "cookie" obtained in using a website*
- ✓ *Information on a consumer report obtained by a financial institution.*[2]

In the Health Care Industry, the Health Insurance Portability and Accountability Act (HIPAA) includes provisions on patient privacy much as GLBA does for financial institutions.

An Internet eMail Questionnaire that can be used for information gathering is included as Appendix B. A Company whose internal eMail system was known to be secure used it to begin documenting their current situation. They found that communications could be broken down into the following categories.

Frequency

- Occasional Business-to-Customer
- Occasional Business-to-Business

These are defined as communications that are not part of the daily processes of a department. They may be individual eMails required to answer an inquiry or request information/service from a vendor on a one-time basis. If a secured solution was not available, these could be accomplished by another means (ie. Fax, Telephone, Secure Website).

- Life of Deal Business-to-Customer
- Life of Deal Business-to- Business

These communications are part of the daily business process of a department. However, the recipients will change as projects or deals are concluded and the next ones started.

- Ongoing Business-to-Customer
- Ongoing Business-to- Business

These are the regularly occurring communications with vendors and business partners that will continue regardless of the completion of a specific deal or

[2] Federal Trade Commission, Bureau of Consumer Protection, Division of Financial Practices "The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information" URL: http://www.ftc.gov/privacy/glbact/glboutline.htm (31 May 2002)

project. As these are long term in nature, these are more suitable to a long-term encryption solution.

- Ongoing Employee-to-Employee

These are the regularly occurring communications between employees within the same company over internal networks. This paper will focus on Internet mail security, however, if a great deal of confidential information is found to be transmitted across internal lines, it might be wise to review the security built into the corporate eMail system.

Data Classification

Once the day-to-day eMail practices in the organization have been documented, it is time to take a look at what is being transmitted and the potential result of interception. As mentioned above, it will be a management decision on balancing cost to risk, however, if the data is classified by sensitivity, it will provide a scale to balance the cost against. Each company must determine its own Data Classification categories and associated risk levels. What follows is a generic example from one company.

4. **Restricted:** Information that is extremely sensitive and is intended for use only by named individuals within the company

3. **Private:** Information that is sensitive within the company and is intended for use only by specified groups of employees, and/or that adds competitive advantage or that can be interpreted as non-public, personal information by government regulation (i.e. *Gramm-Leach-Bliley Act*, HIPPA)

2. **Internal:** Information that is generally available to employees and approved non-employees.

1. **Public:** Non-sensitive information available for external release.

SECURE EMAIL SOLUTIONS

Armed with the information on where the company stands and what its vulnerabilities are, what is available to meet those needs? Current Secure eMail Solutions can be broken down into three categories or a combination of them:

- **Service** eMail is sent and received through a secured site administered by the vendor. There is no need to install anything at the client site.
- **Hardware** An appliance or "Black Box" that is normally installed between the corporate mail server and the firewall to intercept, inspect and process incoming and outgoing eMails
- **Software** The software solution is similar to the hardware solution. Instead of using a "hardened" appliance, the software is loaded onto a corporate server.

The features offered by each type of product may include:

Authentication

The ability to verify that the person opening the message is the person that was intended to receive it. This is normally accomplished through a password.

Message Integrity

The ability to verify that the message is not changed by anyone during the transmission from point A to point B.

Non-Repudiation

The ability to verify that the sender is who they claim to be and that it was their intention to send this message to the recipient.

Firewall

Like the mental picture it brings to mind, a Firewall is a method of protecting the internal mail network from external attack.

Intrusion Detection (Ingress & Egress logging)

The ability to detect and report unusual activity that may be indicative of an attack from the outside or one being initiated from internally against someone else.

Anti-Virus

This feature provides the ability to scan all incoming messages and attachments for viruses, worms, Trojan horses, etc. It should be able to stop, quarantine and/or delete as necessary. As those that perpetrate this kind of foul play are constantly getting better at it, the ability to update virus definitions easily is important.

Anti-Spam

This feature provides the ability to stop incoming and outgoing Spam. SPAM is junk eMail sent in large volumes. It can be used as a form of attack to bring a server down based on it's inability to handle the volume or it could be a marketing campaign where someone was able to get a corporate eMail list. An employee that is trying to make use of the corporate eMail system for his or her own business purposes can also generate SPAM internally. Perhaps they bought into one of the get rich quick schemes that float around in cyber-world and believe they really should send it to every list they can identify (In spite of this being strictly prohibited in the corporate eMail policy.) Regardless of the reason, this is usually detrimental to the functioning of the system.

Policy Manager

The policy manager allows Information Security to set limits on who can send what to whom, whether or not Authentication, Message Integrity, Non-repudiation, or Encryption is required based on sender, recipient, and content among other things.

Confidentially - eMail Encryption

EMail encryption is used to "encode your messages, which are then decoded by the recipient after delivery. Even if the message is viewed in transit by someone else, they will not be able to decipher it."[3]

DEFINING THE REQUIREMENTS

The ideal secure eMail solution for each company will differ based on many factors. Some of the considerations that must be taken into account include:

Vendor

2. Single Source or Multiple Vendors to meet differing needs
3. Pricing model: Per seat, by volume, flat rate, combination
4. Vendor History: Proven reliability and performance or Brand new with latest technology

[3] Higginbotham, Peter. "Introduction to Security Issues in Email – PGP, S/MIME and SSL." Oxford University Computing Services (13 April 2002) http://www.oucs.ox.ac.uk/email/secure (10 May 2002)

General Product

1. Ease of use for employees and whether it works seamlessly with existing corporate eMail system.
2. Attachment capability: number, file size, encryption.
3. Method of notification to client workstation (end user) that message is available for pickup
4. Automatic redirection to a secure SSL server for document retrieval
5. Notification brings end user directly to document
6. Storage of documents on a secure server
7. Software or hardware required by recipient to access and read the secure eMail.
8. The process should be as simple and easy as possible to read in order to avoid customer issues
9. Level of management reporting to provide analysis of the process usage and effectiveness.

Features

1. Authentication
2. Message Integrity
3. Non-Repudiation
4. Firewall
5. Intrusion Detection (Ingress & Egress logging)
6. Anti-Virus
7. Anti-Spam
8. Policy Manager
9. eMail Encryption
   - Business to Business
   - Business to Client
   - Client to Business

Encryption

1. End user replies should also be encrypted.
2. Level of Security
3. What type of Encryption
4. Can the eMail be encrypted between any two points or only between someone else who has the same solution?
5. Are the message and any attachments encrypted or only the message?
6. If dealing internationally, does the product conform to government

regulations?

WHAT IS CURRENTLY ON THE MARKET

> *Current Solutions are limited. Currently, a number of solutions such as email proxy gateways, email message encryption (e.g., S/MIME or PGP) or email virus scanning software are available to minimize email security risks. While each of these tools to varying degrees, can improve your security, can improve your security posture, they are piecemeal and fail to address the overall security risks of email systems. For the most part, these current solutions serve merely as "speed-bumps" for intruders and they frequently lead to a false sense of security.*[4]

While this statement may leave the IT professional feeling there is very little hope for securing their eMail system, the reality of the situation is not as alarming as that. There are many products currently available that fulfill a segment of the need, but few that are all encompassing.

Begin your search by focusing on the most critical features to your organization. In the case of the financial institution that was conducting this the two most important features were found to be: 1) Seamless integration with the corporate eMail system and 2) the ability to communicate with customers, prospects and vendors that were not necessarily security literate and would probably not have the ability to receive encrypted messages.

The Appendix A - Vendors List provides the names and contact information for those vendors that we believed offered the features that we determined were necessary to implement a Secure eMail Solution.

The next phase for our company was to proceed with a Request for Information from the vendors believed to provide the best fit and to bring the top three into our test lab. We are currently performing final evaluations of SRA Int'l – Assentor & Tovaris, Tumbleweed Communications Corp. and ZixIt Corporation.

CONCLUSION

[4] CipherTrust White Paper, "Understanding and Responding to Email System Risks," Page 5

Now when the eventual management question, “Is our eMail secure?” gets asked, you have the framework to prepare a management report of Business Need based on Frequency, Volume and Content with a ballpark estimate of costs to secure any needed avenues of communication.

At the time we completed this portion of our project, May 2002, the estimate was $30,000 - $225,000 with implementation in two - four months from the time the vendor was chosen

It is important to remember this is a rapidly evolving technology. There are products available today that were unheard of six months ago. One can only assume that six months from now, even more robust products will become available.

REFERENCES

CipherTrust White Paper, "Understanding and Responding to Email System Risks,"

Ellison, Carl. Bruce Schneier, "Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure." http://www.counterpane.com/pki-risks-ft.txt (5 May 2002)

Federal Trade Commission, Bureau of Consumer Protection, Division of Financial Practices. "The Gramm-Leach-Bliley Act Privacy of Consumer Financial Information" 18 June 2001. http://www.ftc.gov/privacy/glbact/glboutline.htm (31 May 2002)

Fontana, John. "So Much for Secure eMail." NetworkWorldFusion News. 13 Aug 2001. http://www.nwfusion.com/archive/2001/123782_08-13-2001.html (15 May 2002)

Foundation for Information Technology Education. "AITP Model Electronic Mail (E-mail) Policy." http://www.edfoundation.org/ef2001/emailpolicy.htm (10 May 2002)

GFI Software Ltd. White Paper. "Why you need GFI MailSecurity ." http://www.gfi.com/mailsecurity/wpwhygfimsec.htm (5 May 2002)

GFI Software Ltd. White Paper. "eMail Encryption." http://www.gfi.com/mailsecurity/wpemailsecurity.htm (5 May 2002)

Higginbotham, Peter. "Introduction to Security Issues in Email – PGP, S/MIME and SSL." Oxford University Computing Services (13 April 2002) http://www.oucs.ox.ac.uk/email/secure (10 May 2002)

Isaacs, Margaret. "Security and Encryption -- Secure email." Terena Guide to Network Resource Tools. 21 Aug 2002. http://www.terena.nl/libr/gnrt/security/s4.html (16 Sep 2002)

Ries, David G. "Attorney Confidential Communications by eMail" Cyberspace Lawyer. Vol. 6 No. 6 (2001): 4-10

Whitten, Alma. J. D. Tygar. "Why Johnny Can't Encrypt," 23 Aug 1999. http://www-2.cs.cmu.edu/~alma/johnny.pdf (10 May 2002)

APPENDIX A - VENDORS LIST

CipherTrust IronMail
1105 Sanctuary Parkway, Suite 450
Alpharetta, GA 30004
877.448.8625
www.ciphertrust.com

Net Delivery – MsgStream
4725 Walnut Street
Boulder, CO 80301
303.245.1000
www.netdelivery.com

PostX
3 Results Way
Cupertino, CA 95014-9524
408.861.3500
www.postx.com

PrivateExpress,Inc.
3190 Clearview Way, Suite 100
San Mateo, CA 94402
888.964.2700
www.privateexpress.com

Sigaba Corporation
2727 S. El Camino Ral
San Mateo, CA 94403
650.572.6100
www.sigaba.com

SRA Int'l – Assentor & Tovaris
4300 Fair Lakes Court
Fairfax, VA 22033
703.80.1500
www.assentor.com

Tovaris
213 E. Water Street
Charlottesville, VA 22902
434.245.5300
www.tovaris.com

Tumbleweed Communications Corp.
700 Saginaw Drive
Redwood City, CA 94063
650.216.2000
www.tumbleweed.com

VeriSign Worldwide Headquarters
487 East Middlefield Road
Mountain View, CA 94043
650-961-7500
www.verisign.com

ZixIt Corporation
2711 N. Haskell Ave.,
Suite 2850, LB 36
Dallas, TX 75204-2911
214-515-7300
www.zixit.com

APPENDIX B - INTERNET E-MAIL QUESTIONNAIRE

Today, several departments at <company> use Internet e-mail to conduct business. These departments have grown to rely on this efficient channel for both internal and external communication. The security of e-mail is not the same as the U.S. Post Office or other more traditional methods of communication. Therefore, information must be gathered to define the current e-mail practices.

This questionnaire will be used to conduct an analysis of various e-mail practices. This information will provide the foundation for a recommended approach to securing e-mails.

There may be several different solutions to the e-mail issue, so the questions relate to the types of e-mails sent as well as questions to the party communicated with. Please help in this effort by completing the chart for as many instances as you can define that meet the following criteria:

- **Internet E-mails that include customer information that is private to the <company> (not public)**
- **Internet E-mails that include information related to the <company> that the <company> would not want to have displayed publicly without its knowledge**

1. Complete this chart if your department sends e-mails via the Internet that are short-term, temporary communications that also fit the bolded criteria above. (Examples of this include an e-mail to a customer regarding a "deal" such as mortgage, loan, etc. After the deal is done, the e-mails cease.)

Recipient (customers, vendor, etc.)	Content	Frequency & Volume (#/day, #/week, etc.)	Duration (Once, weeks, etc.)

2. Complete this chart if your department sends e-mails via the Internet that are longer-term, established communications. (Examples of this include e-mails to a vendor or third-party with whom the Bank has a continuing relationship.)

Recipient (customers, vendor, etc.)	Content	Frequency & Volume (#/day, #/week, etc.)	Term of the relationship (3 months, 1 year, indefinite, etc.)
